Categoria Documento: Politica	Identificazione Documento: **PO-01**

Politica per la qualità e la sicurezza delle informazioni del SCT di Regione Toscana

REVISIONI DEL DOCUMENTO		
Data	**Elenco Modifiche**	**Approvato**
2014-09-17	Politica emessa in conformità a ISO/IEC 27001:2015	Laura Castellani
2015-10-08	Estensione a conservazione sostitutiva	Laura Castellani
2018-01-12	Aggiornamento per conservazione sostitutiva	Laura Castellani
2019-06-11	Aggiornamento per servizi cloud (ISO/IEC 27017 e 27018)	Angelo Marcotulli
2019-07-03	Aggiornamento per qualità (ISO 9001 e ISO 22301)	Angelo Marcotulli
2019-10-23	Correzioni e nuova approvazione	Sergio Papiani
2020-04-29	Riferimenti contratto conservazione	Sergio Papiani
2021-01-21	Riferimenti a proroga tecnica per 2021	Sergio Papiani
2021-10-01	Aggiornamento sui contratti di fornitura del servizio a RT	Sergio Papiani
2022-06-14	Riesame complessivo per adeguamento al Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici di AgID.	Sergio Papiani

Il contenuto del presente documento è riservato ad uso di Regione Toscana e del gestore SCT

SOMMARIO

1 Politica per la qualità e la sicurezza delle informazioni.....3

2 Politica per la qualità e per la sicurezza delle informazioni relativa alla conservazione dei documenti informatici.....5

Il contenuto del presente documento è riservato ad uso di Regione Toscana e del gestore SCT

1 POLITICA PER LA QUALITÀ E LA SICUREZZA DELLE INFORMAZIONI

Il SCT è un'infrastruttura della Regione Toscana che offre servizi di:

- centro servizi e centro tecnico di supporto per i soggetti pubblici costituenti la Rete Telematica Regionale Toscana; ospita il "cloud computing" di RT, offrendo agli utenti anche soluzioni di tipo IaaS e PaaS;
- un punto di interscambio tra le reti degli operatori Internet commerciali (Internet Service Provider) e le reti della Pubblica Amministrazione anche in linea con i requisiti SPC.

Il quadro di riferimento per fissare gli obiettivi della Qualità e della Sicurezza delle Informazioni prevede le seguenti direttrici:

1. Consolidare il data center in Cloud di Regione Toscana rendendolo capace di accogliere le esigenze della PA di tutto il territorio rendendo disponibili piattaforme abilitanti per lo sviluppo e l'evoluzione di servizi;
2. Migliorare, tramite il Cloud e le piattaforme abilitanti su di esso disponibili, i servizi della PA per i cittadini e le imprese, con l'obiettivo di continuare ad innovare la PA, migliorare il livello di digitalizzazione, di semplificazione, di garantire i diritti di cittadinanza digitale e di accesso on line ai servizi e favorire di fatto i processi di transizione al digitale, richiesti alla PA.
3. Mantenere e migliorare un sistema che consenta all'Ente attivo sul sistema di inviare in conservazione documenti per le tipologie documentali di proprio interesse, secondo le modalità scelte, e ne gestisca anche il ciclo di vita;
4. Mantenere e migliorare un sistema che consenta di conservare la documentazione inviata dagli Enti secondo la normativa vigente;
5. Mantenere e migliorare un sistema che consenta all'Ente di ricercare, verificare lo stato della documentazione presente sul sistema e richiederne ed ottenerne l'esibizione.

Nell'infrastruttura di SCT sono gestiti, tra gli altri: i dati dei cittadini (dati sanitari incluso il FSE, dati di pagamento e i dati delle imprese); i dati della Regione stessa (archiviazione sostitutiva, le piattaforme di e-procurement, database DBRMS); i dati di "clienti" della Regione Toscana a cui è offerto il servizio di hosting e le infrastrutture di interscambio.

Per questa gestione (o trattamento), è fondamentale che i servizi siano offerti con attenzione alla Qualità e alla Sicurezza delle Informazioni.

Questo si traduce nella salvaguardia dei seguenti parametri:

- riservatezza: le informazioni non devono essere accessibili a entità non autorizzate (fondamentale per i dati sanitari, per l'e-procurement);
- integrità: le informazioni non devono essere modificate da entità non autorizzate, non devono essere corrotte e devono essere affidabili (fondamentale per i dati dell'Amministrazione, per l'e-procurement e per i dati sanitari);

Il contenuto del presente documento è riservato ad uso di Regione Toscana e del gestore SCT

- disponibilità: le informazioni devono essere accessibili alle entità autorizzate nei tempi previsti (fondamentale per le operazioni del punto di interscambio e per l'e-procurement).

Obiettivo è mantenere e migliorare un "Sistema Cloud Toscana" (SCT) in grado di garantire i necessari e indispensabili parametri di continuità e affidabilità in una logica di forte interoperabilità e sistematicità. Il sistema è fisicamente costituito da un nodo primario, il Data Center TIX, e da almeno un nodo secondario, deputato ad assicurare il Disaster Recovery del sito primario e la continuità applicativa dei servizi identificati come critici. Per questo è necessario prevedere un sistema di gestione per la continuità operativa come strumento fondamentale dal punto di vista organizzativo al fine di assicurare la continuità operativa delle operazioni indispensabili per i servizi erogati dal Data Center SCT e il ritorno alla normale operatività in caso di disastro.

È altresì necessario che sia rispettata la normativa vigente applicabile alle operazioni del SCT (in particolare quella relativa alla protezione dei dati personali) e relativa all'Amministrazione digitale, agli appalti, alla sicurezza e igiene dei lavoratori e alla privacy a livello statale, regionale e delle autorità quali AgID. Dovranno anche essere rispettati gli accordi sottoscritti in materia con gli altri soggetti pubblici e privati ai quali Regione Toscana eroga servizi.

Quanto sopra indicato rappresenta il valore che Regione Toscana offre attraverso i servizi offerti: qualità, continuità e sicurezza dei servizi, rispetto della normativa vigente e trasparenza. Dall'altra parte, Regione Toscana ottiene, come valore, un migliore servizio ai cittadini e un più attento controllo dei costi dell'infrastruttura informatica.

Regione Toscana ha quindi deciso di dotare il SCT di un sistema di gestione per la sicurezza delle Informazioni conformi gli standard internazionali ISO/IEC 27001 (con le relative integrazioni per ISO/IEC 27017 e ISO/IEC 27018) che le permetterà di:

- dare le opportune garanzie alle parti interessate (cittadini, imprese operanti nel territorio, altre amministrazioni, operatori di telecomunicazioni);
- governare efficacemente i fornitori e outsourcer coinvolti nella gestione del SCT;
- migliorare il livello di sicurezza delle informazioni trattate anche attraverso il processo di gestione degli incidenti e delle vulnerabilità;
- monitorare la qualità dei servizi erogati.

Il sistema di gestione per la qualità e la sicurezza delle informazioni conforme ai requisiti della ISO 9001 e della ISO/IEC 27001 è applicato:

- alla governance delle infrastrutture fisiche del SCT;
- alla governance relativa alla gestione delle operazioni a livello sistemistico (servizi di housing, hosting, gestione e monitoraggio sistemi e della rete, Infrastructure as a Service, Platform-as-a-Service, Software-as-a-Service).

La presente Politica prende in considerazione, oltre al Codice in materia di protezione dei dati personali e quindi alla conformità di quanto previsto nel Reg. 2016/679/UE, le linee guida ISO/IEC 27017, relativa ai controlli integrativi per i clienti ed i fornitori di servizi in cloud e le linee guida ISO/IEC 27018, relativa ai controlli per i Responsabili del trattamento e per i fornitori di servizi in cloud. In particolare:

Il contenuto del presente documento è riservato ad uso di Regione Toscana e del gestore SCT

- le informazioni archiviate nell'ambiente di cloud computing sono soggette all'accesso e alla gestione da parte del fornitore di servizi cloud;
- le risorse (gli applicativi) sono mantenute nell'ambiente di cloud computing;
- i processi sono eseguiti su un servizio cloud virtualizzato e multi-tenant;
- gli accordi contrattuali con i fornitori dei servizi cloud sono redatti definendo chiaramente le responsabilità sul trattamento dei dati nel cloud e rappresentano eventuali riferimenti e responsabilità di sub-appaltatori.

Gli obiettivi annuali di qualità e sicurezza delle informazioni per il SCT di Regione Toscana sono riportati nel Riesame di direzione.

I principi cardine a cui attenersi per garantire un adeguato livello di sicurezza per i dati trattati sono i seguenti:

- le informazioni sono accessibili solo a coloro che ne hanno necessità (principio need to know);
- il personale è opportunamente formato in materia di qualità e sicurezza delle informazioni in maniera tale da seguire la normativa applicabile e le regole e politiche interne;
- i fornitori sono opportunamente controllati, secondo quanto applicabile, attraverso clausole contrattuali, audit, monitoraggio, condivisione di report e di azioni di miglioramento;
- i dati sono trattati solo per le finalità dichiarate agli interessati o agli enti;
- nei progetti, interni e per i clienti, si considerano i requisiti di sicurezza e di qualità sin dalla loro ideazione, nonché nella progettazione dei prodotti e durante tutta l'erogazione dei servizi;
- sono stabiliti i requisiti di base per la progettazione dei servizi (cloud e non cloud), anche considerando che:
  - ai servizi hanno accesso più enti cliente e che i dati di ciascuno devono essere segregati;
  - gli accessi devono essere differenziati per gli utenti e gli amministratori e devono assicurare la robustezza dei meccanismi di identificazione e autenticazione e il controllo degli accessi ai dati anche da parte degli amministratori;
  - i meccanismi di virtualizzazione devono essere configurati in modo sicuro;
- ogni opportunità di miglioramento è individuata e analizzata affinché possa essere colta e permetta di offrire servizi sempre più adatti ai propri clienti;
- i rischi di sicurezza delle informazioni e quelli di qualità, inclusi quelli originati da personale interno, sono identificati, analizzati, valutati e trattati al fine di prevenirli o ridurne gli impatti, considerandone anche gli impatti economici e i vincoli imposti per la Pubblica amministrazione;

Il contenuto del presente documento è riservato ad uso di Regione Toscana e del gestore SCT

- gli enti cliente vanno preavvertiti di cambiamenti con impatti significativi;
- la gestione degli incidenti deve essere in linea con quanto stabilito dalla normativa vigente e dalle necessità di raccolta di prove legali.

Questa politica del sistema di gestione per la qualità e la sicurezza delle informazioni, affinché sia efficace, è accompagnata da linee guida più dettagliate su tematiche rilevanti e comunicata a tutto il personale di Regione Toscana e ai fornitori coinvolti nella gestione del SCT. Inoltre, per assicurarne l'adeguatezza nel tempo, sarà riesaminata annualmente a seguito di una completa valutazione del rischio.

2 POLITICA PER LA QUALITÀ E PER LA SICUREZZA DELLE INFORMAZIONI RELATIVA ALLA CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Regione Toscana ha come missione quello di essere il polo archivistico per tutta la Regione e di promuovere lo sviluppo della società dell'informazione e della conoscenza (Leggi regionali 1 del 2004 e 54 del 2009).

Pertanto, tra i servizi offerti dal SCT, vi è quello di conservazione dei documenti informatici, rivolto agli enti locali e a Regione Toscana stessa in conformità a quanto pubblicato da AgID relativo al "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici" del dicembre 2021.

I dati che il servizio è destinato a conservare possono essere quindi molto critici e di elevato valore per la Pubblica Amministrazione. In alcuni casi possono essere "particolari" secondo la definizione riportata nel GDPR.

La conservazione dei documenti informatici rispetta i requisiti attraverso:

- scelte tecnologiche destinate a questo scopo (formati dei dati, delle firme e delle marche temporali; scalabilità delle soluzioni scelte);
- scelta di fornitori affidabili e con contratti che considerano la necessità di conservazione a lungo termine (incluso il controllo delle licenze);
- verifiche periodiche dei supporti fisici utilizzati, dell'adeguatezza del software e degli altri sistemi pertinenti e dell'integrità e disponibilità dei dati, della capacità dei sistemi;
- il controllo dei cambiamenti di organizzazione, processi e tecnologia, anche attraverso incontri periodici con le parti interessate all'erogazione del servizio (Regione Toscana, gestore IT, esercizio applicativo);
- la verifica della normativa applicabile.

Per questo Regione Toscana si avvale di:

- SCT per ospitare l'hardware e gestire parte dei sistemi e la rete (ex TIX);
- un fornitore scelto specificamente, già accreditato per questo servizio, per la progettazione e il mantenimento del software, per la conduzione applicativa e dei sistemi coinvolti.

I principi di qualità e di sicurezza espressi nella politica generale rimangono validi e sono dettagliati nelle specifiche procedure del sistema di gestione per la qualità e per la sicurezza delle informazioni.

Per il mantenimento del sistema sono definiti i seguenti ruoli:

Il contenuto del presente documento è riservato ad uso di Regione Toscana e del gestore SCT

- Responsabile del servizio di conservazione;
- Responsabile della funzione archivistica di conservazione;
- Responsabile del trattamento dei dati personali;
- Responsabile della sicurezza dei sistemi per la conservazione;
- Responsabile dei sistemi informativi per la conservazione;
- Responsabile dello sviluppo e della manutenzione del sistema di conservazione.

Questa politica è:

- messa a disposizione su Start agli enti produttori in occasione di ogni modifica;
- messa a disposizione sulla pagina “Agenda digitale Toscana” (pagina DAX) e sul sito di Cloud Toscana;
- consegnata ai fornitori.

Il contenuto del presente documento è riservato ad uso di Regione Toscana e del gestore SCT